Securing Your Web Browser

Will Dormann and Jason Rafail
US-CERT

Summary

This paper will help you configure your web browser for safer internet surfing. It is written for home computer users, students, small business workers, and any other person who works with limited Information Technology (IT) support and broadband (cable modem, DSL) or dial-up connectivity. Although the information in this document may be applicable to users with formal IT support as well, organizational IT policies should supersede these recommendations.

Why Secure Your Web Browser?

Today, web browsers such as Internet Explorer, Mozilla Firefox, and Safari (to name a few), are installed on almost all computers. Because web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead quickly to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer.

Ideally, computer users should evaluate the risks from the software they use. Many computers are sold with software already loaded. Whether installed by a computer manufacturer, operating system maker, internet service provider, or by a retail store, the first step in assessing the vulnerability of your computer is to find out what software is installed and how one program will interact with another. Unfortunately, it is not practical for most people to perform this level of analysis.

There is an increasing threat from software attacks that take advantage of vulnerable web browsers. In recent months, US-CERT has observed a trend whereby new software vulnerabilities are exploited and directed at web browsers through the use of compromised or malicious web sites. This problem is made worse by a number of factors, including the following:

- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities may have been discovered since the software was configured and packaged by the manufacturer.
- Many web sites require that users enable certain features or install more software, putting the computer at additional risk.

- Many users do not know how to configure their web browsers securely.
- Many users are unwilling to enable or disable functionality as required to secure their web browser.
- Many users are unaware whether or not their computer has been compromised.
- Many users fail to properly “clean” a compromised computer.

As a result, exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems.

In addition to following this paper's recommendations, refer to the documentation in the References section for other steps you can take to secure your computer.

Understanding Web Browser Features

It is important to understand the functionality and features of the web browser you use. Enabling some web browser features may lower security. For example, the ActiveX software feature has a history of vulnerabilities that have lead to severe security impacts when enabled.

Multiple web browsers may be installed on your computer. Other software applications on your computer, such as email clients or document viewers, may use a different browser than the one you normally use to access the web. Also, certain file types may be configured to open with a different web browser. Using one web browser to access web sites does not mean other applications will automatically use the same browser. For this reason, it is important to securely configure each web browser installed on your computer.

Web sites may require the use of a browser that supports scripting or active content, such as JavaScript or ActiveX controls, or the sites themselves may contain vulnerabilities. Web sites can be considered products, and as a user of the product, you can contact the web site administrators and request that the sites be designed so that they do not require the use of features that may pose a computer security risk.

Some specific web browser features and attributes are described in this document. Understanding what different features do will help you understand how they affect your web browser's functionality and the security of your computer.

ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or may download the component from a web site. This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented.

Java is an object-oriented programming language that can be used to develop active content for web sites. A Java Virtual Machine, or JVM, is used to execute the Java code, or "applet," provided by the web site. The JVM is designed to separate, or "sandbox," running code so that it does not affect the rest of the system. Some operating systems come with a JVM, while others require a JVM to be installed before Java can be used. Java applets run independently from the operating systems.

Active Content, or plug-ins, are intended for use in the web browser. They are similar to ActiveX controls but cannot be executed outside of a web browser. Macromedia Flash is an example of Active Content that can be provided as a plug-in.

JavaScript is a dynamic scripting language that is used to develop active content for web sites. Unlike Java, JavaScript is a language that is interpreted by the web browser directly. There are specifications in the JavaScript standard that restrict certain features such as accessing local files.

VBScript is a programming language that is unique to Microsoft Windows. VBScript is similar to JavaScript, but it is not as widely used in web sites because of its limited compatibility with browsers other than Internet Explorer.

Cookies are text files placed on your compute to store data that is used by a web site. A cookie can contain any information that a web site is designed to place in it. Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site. Cookies are designed to be readable only by the web site that created them.

Security Zones and the Domain Model are methods Microsoft Windows uses designed to provide multiple levels of security settings for a single system. While primarily used by Internet Explorer, it can be invoked by other applications on the system that use components of Internet Explorer. You can learn more about Microsoft's Security Zones, the Domain Model, and how to secure them at this web site:
http://www.microsoft.com/windows/ie/using/howto/security/setup.asp.

Vulnerabilities and Attack Vectors

Increasingly, attackers are exploiting client-side systems (your computer) through various vulnerabilities. They use these vulnerabilities to take control of your computer, steal your information, destroy your files, and attack other computers. A low-cost way for attackers to gain control of your computer is by exploiting vulnerabilities in web browsers. An attacker can simply create a malicious web page that will install Trojan software or spyware that will steal information from your computer. Additional information about spyware is available in the following document: http://www.us-cert.gov/reading_room/spyware.pdf. Rather than actively targeting and attacking vulnerable systems, a malicious web site can passively compromise systems as the site is visited. A malicious HTML document can also be emailed to victims. In these cases, the act of opening the email or attachment can compromise the system.

In this section, we will point out some common vulnerabilities in web sites and web browsers that tend to be exploited. We will not go into great detail in this document, but will provide links to other documentation that will help explain the vulnerabilities.

ActiveX Controls

ActiveX is a technology that has been plagued with various vulnerabilities and implementation issues. One problem with using ActiveX in a web browser is that it greatly increases the attack surface, or "attackability," of a system. Vulnerabilities in ActiveX objects may be exploited via Internet Explorer, even if the object was never designed to be used in a web browser. In 2000, the CERT/CC[1] held a workshop to analyze security in ActiveX. The results from that workshop may be viewed here: http://www.cert.org/reports/activeX_report.pdf. Many vulnerabilities associated with ActiveX controls lead to severe impacts. Attackers exploiting ActiveX vulnerabilities can frequently take control of computers. You can search the US-CERT and CERT/CC web sites for ActiveX vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=activex and http://search.cert.org/query.html?qt=activex.

Java

Java is an object-oriented programming language developed by Sun Microsystems. A Java applet is machine-independent[2] and requires a Java Virtual Machine (JVM) on the client computer so that it can execute. Java applets traditionally execute within a "sandbox" where the interaction with the rest of the system is limited. However, various implementations of the JVM contain vulnerabilities that allow an applet to bypass these restrictions. Signed Java applets can also bypass sandbox restrictions, but they generally prompt the user before they can execute. You can search the US-CERT and CERT/CC web sites for Java vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=java
and http://search.cert.org/query.html?col=certadv&col=vulnotes&qt=java.

Cross-Site Scripting

Cross-site scripting, often referred to as CSS or XSS, is a vulnerability in a web site that permits an attacker to leverage the trust relationship that you have with that site. For a high-level description of CSS attacks, please read the whitepaper published at http://www.cert.org/archive/pdf/cross_site_scripting.pdf. Note that cross-site scripting is not usually caused by a failure in the web browser. You can search the CERT/CC web sites for cross-site scripting vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=java and http://search.cert.org/query.html?qt=cross-site+scripting.

1 CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.
2 Machine-independent software can run on many types of computers.

Cross-Zone and Cross-Domain Vulnerabilities

Most web browsers employ security models to prevent a web site from accessing data in a different domain. These security models are primarily based on the Netscape Same Origin Policy: http://www.mozilla.org/projects/security/components/same-origin.html. Internet Explorer also has a policy to enforce security zone separation: http://msdn.microsoft.com/workshop/security/szone/overview/overview.asp.

Vulnerabilities in these security models can be used to perform actions that a site could not normally perform. The impact can be similar to a cross-site scripting vulnerability. However, if a vulnerability allows for an attacker to cross into the local machine zone or other protected areas, the attacker may be able to execute arbitrary commands on the vulnerable system. You can search the US-CERT and CERT/CC web sites for cross-zone and cross-domain vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=cross-domain and http://search.cert.org/query.html?qt=cross-domain.

Malicious Scripting, Active Content, and HTML

Some sites may contain malicious scripts, active content, or HTML that will attempt to trick the visitor into providing information, or performing an action that will enable the attacker to gain some privilege. In the absence of vulnerabilities, the attackers rely on social engineering to gain access to the victim's information. However, vulnerabilities in web browsers may be exploited to gain privileges as well. Below is a list of vulnerabilities in web browsers that may provide an exploit vector through the use of malicious code. In 2000, the CERT/CC released a frequently asked questions (FAQ) document on malicious scripting. It is available here: http://www.cert.org/tech_tips/malicious_code_FAQ.html. You can search the US-CERT and CERT/CC web sites for malicious scripting and content vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=malicious+scripting+active+content and http://search.cert.org/query.html?qt=malicious+scripting+active+content.

Spoofing

As it relates to web browsers, spoofing is a term used to describe methods of faking various parts of the browser user interface. This may include the address or location bar, the status bar, the padlock, or other user interface elements. Phishing attacks often utilize some form of spoofing to help convince the user to provide personal information. If a user's browser is vulnerable to spoofing, they are more likely to fall victim to a phishing attack. You can search the US-CERT and CERT/CC web sites for malicious scripting and content vulnerabilities at the following URLs: http://search.us-cert.gov/query.html?qt=browser+spoof and http://search.cert.org/query.html?qt=browser+spoof.

The US-CERT document "Technical Trends in Phishing Attacks" (available at http://www.us-cert.gov/reading_room/phishing_trends0511.pdf) has more information about spoofing and phishing techniques.

How to Secure Your Web Browser

Some software features that provide functionality to a web browser, such as ActiveX, Java, Scripting (JavaScript, VBScript, etc), may also introduce vulnerabilities to the computer system. These may stem from poor implementation of the protocol, poor design, poorly written software, or an insecure configuration. For these reasons, you should understand which browsers support which features and the subsequent risks they could introduce. Some web browsers permit you to fully disable the use of these technologies, while others may only permit you to reduce functionality.

This section shows you how to securely configure a few of the most popular web browsers and how to disable features that can cause vulnerabilities. We encourage you to visit the web site for the browser you use to learn more. If a vendor does not provide documentation on how to secure the browser, we encourage you to contact them and ask for it.

Web browsers are frequently updated. Depending on the version of your software, the features and options may move or change.

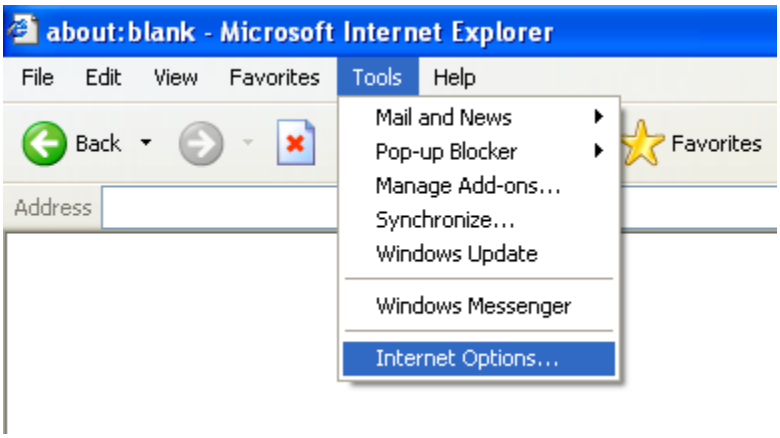
Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is a web browser integrated into the Microsoft Windows operating system. Removal of this application is not practical.

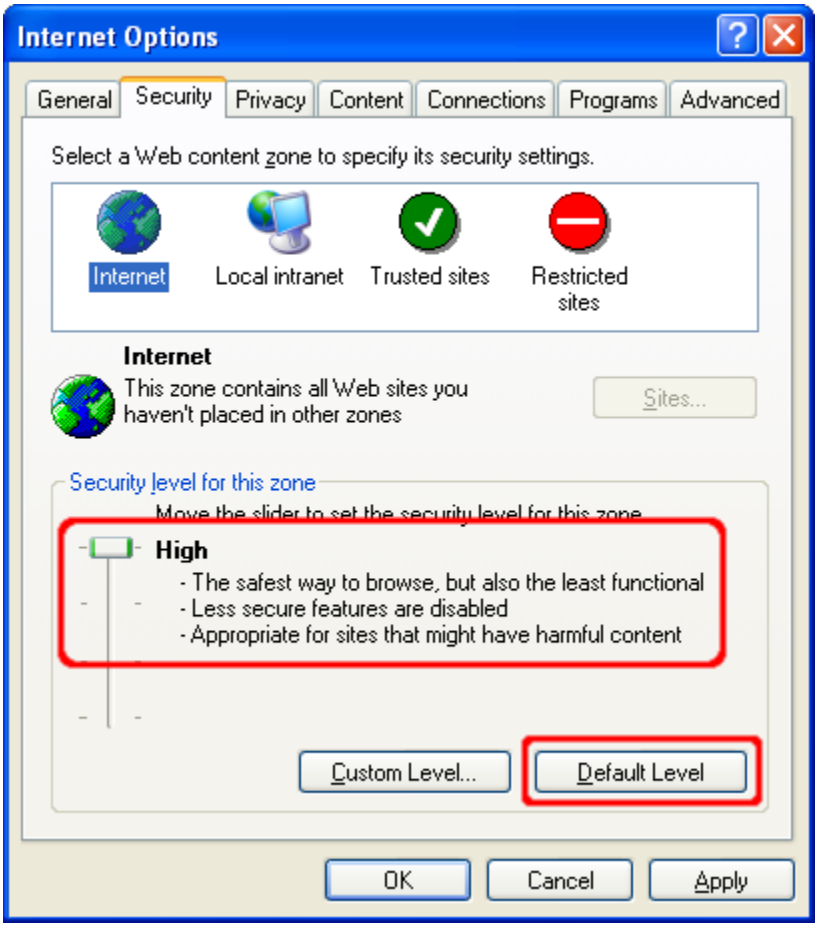
In addition to supporting Java, scripting and other forms of active content, Internet Explorer implements ActiveX technology. While any application is potentially vulnerable to attack, it is possible to mitigate a number of serious vulnerabilities by using a web browser that does not support ActiveX controls. However, using an alternate browser may affect the functionality of some sites that require the use of ActiveX controls. Note that using a different web browser will not remove IE or other Windows components from the system. Other software, such as email clients, may invoke IE, the WebBrowser ActiveX control, or the IE HTML rendering engine (MSHTML). Use of these products may reintroduce the risks presented by these vulnerabilities. Results from the CERT/CC ActiveX workshop in 2000 are available at the following URL: http://www.cert.org/reports/activeX_report.pdf.

Here are steps to disable various features in Internet Explorer. Note that menu options may vary between versions of IE, so you should adapt the steps below as appropriate.

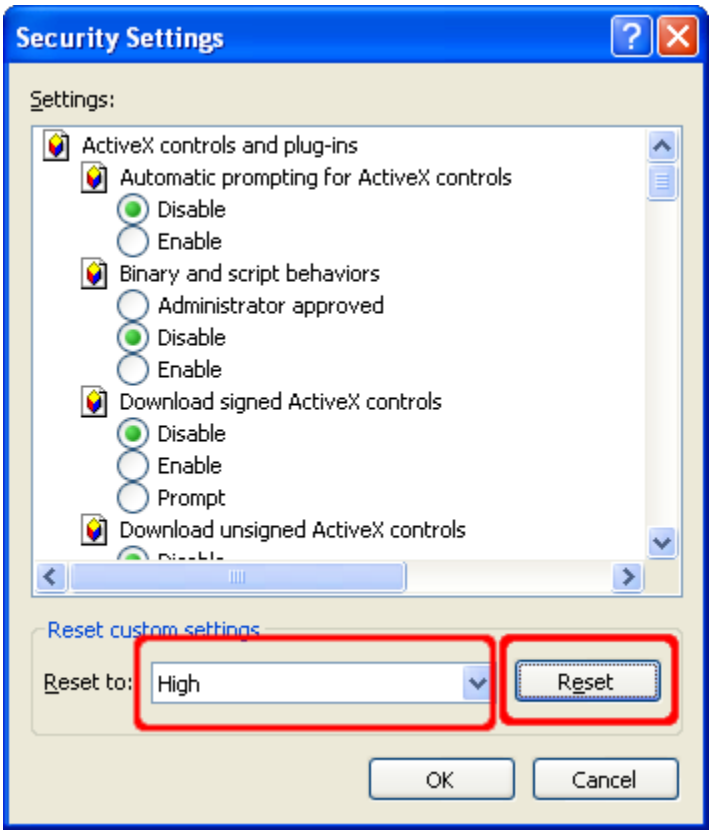
In order to change settings for Internet Explorer, select **Tools** then **Internet Options…**



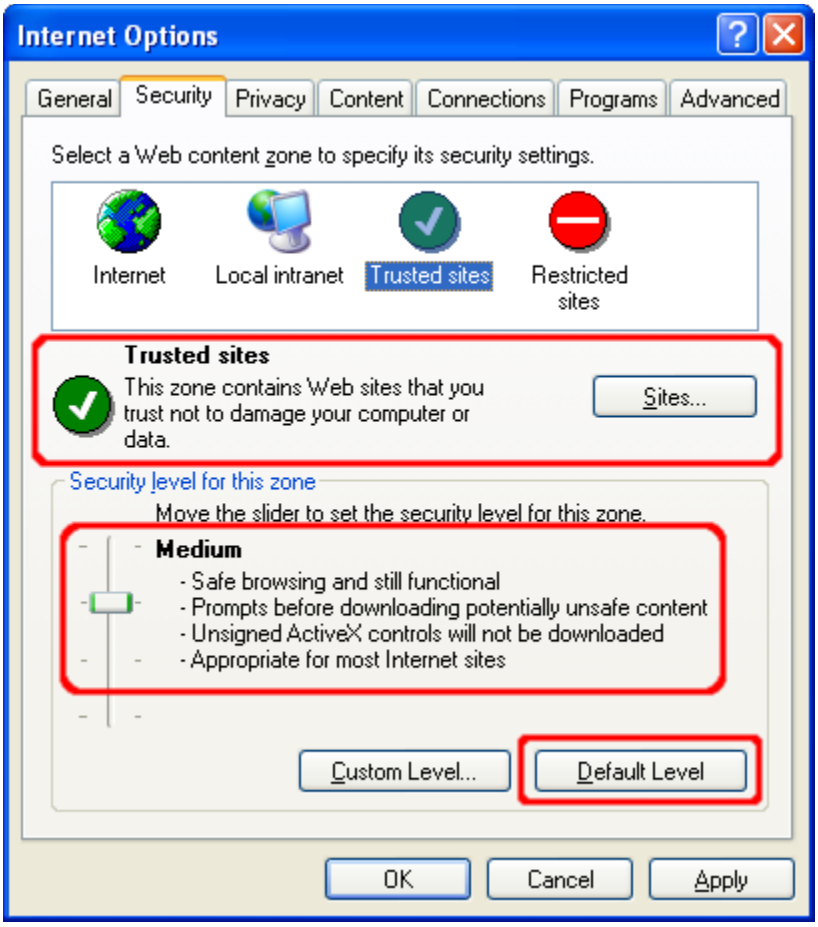
Select the **Security** tab. On this tab you will find a section at the top, which lists the various security zones that Internet Explorer uses. More information about Internet Explorer security zones is available in the Microsoft document Setting Up Security Zones. For each of these zones, you can select a Custom Level of protection. By clicking the **Custom Level** button, you will see a second window open that permits you to select various security settings for that zone. The **Internet** zone is where all sites initially start out. The security settings for this zone apply to all the web sites that are not listed in the other security zones. We recommend the **High** security setting be applied for this zone. By selecting the High security setting, several features including ActiveX, Active scripting, and Java will be disabled. With these features disabled, the browser will be more secure. Click the **Default Level** button and then drag the slider control up to **High**.



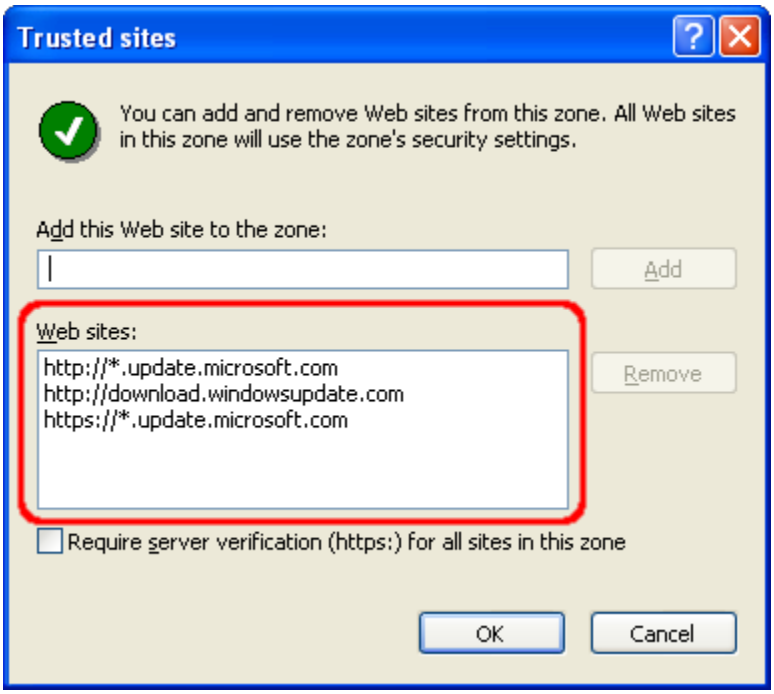
For a more fine-grained control over what features are allowed in the zone, click the **Custom Level** button. Here you can control the specific security options that apply to the current zone. Default values for the High security setting can be selected by choosing **High** and clicking the **Reset** button to apply the changes.



Trusted sites is a security zone for web sites that you believe are securely designed and contain trustworthy content. To add or remove sites from this zone, you can click the **Sites…** button.

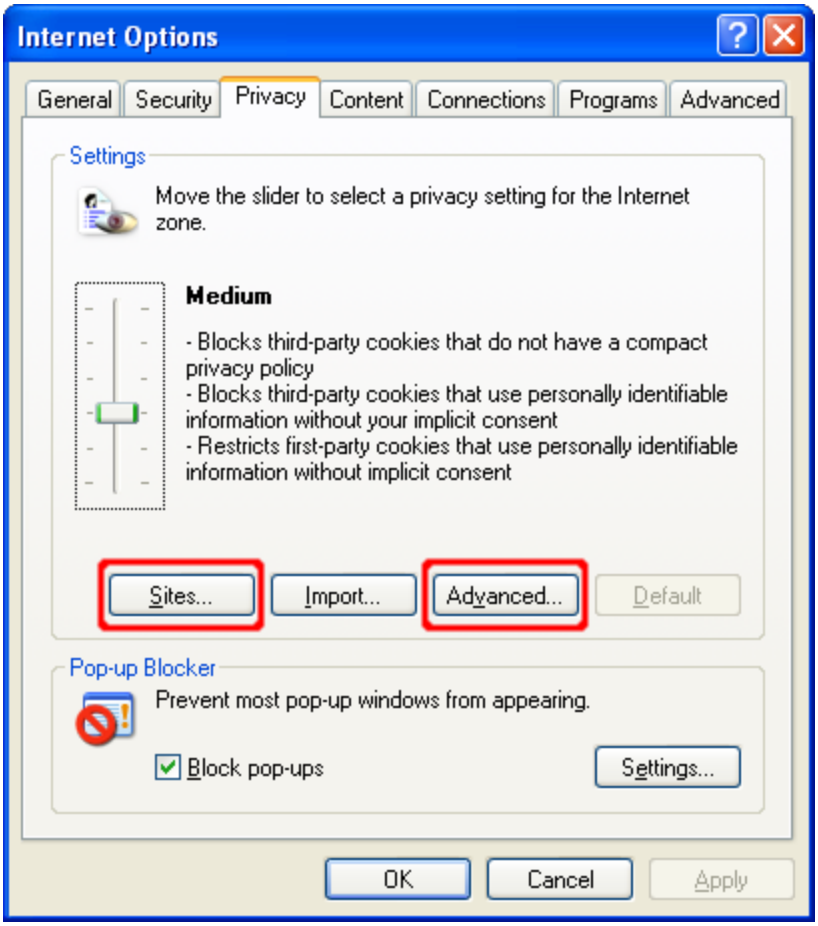


This will open a new window that will list the sites that you trust and permit you to add or remove sites. You may also require that only sites with Secure Sockets Layer (SSL) implemented can be active in this zone. This permits you to verify that the site you are visiting is the site that it claims to be.



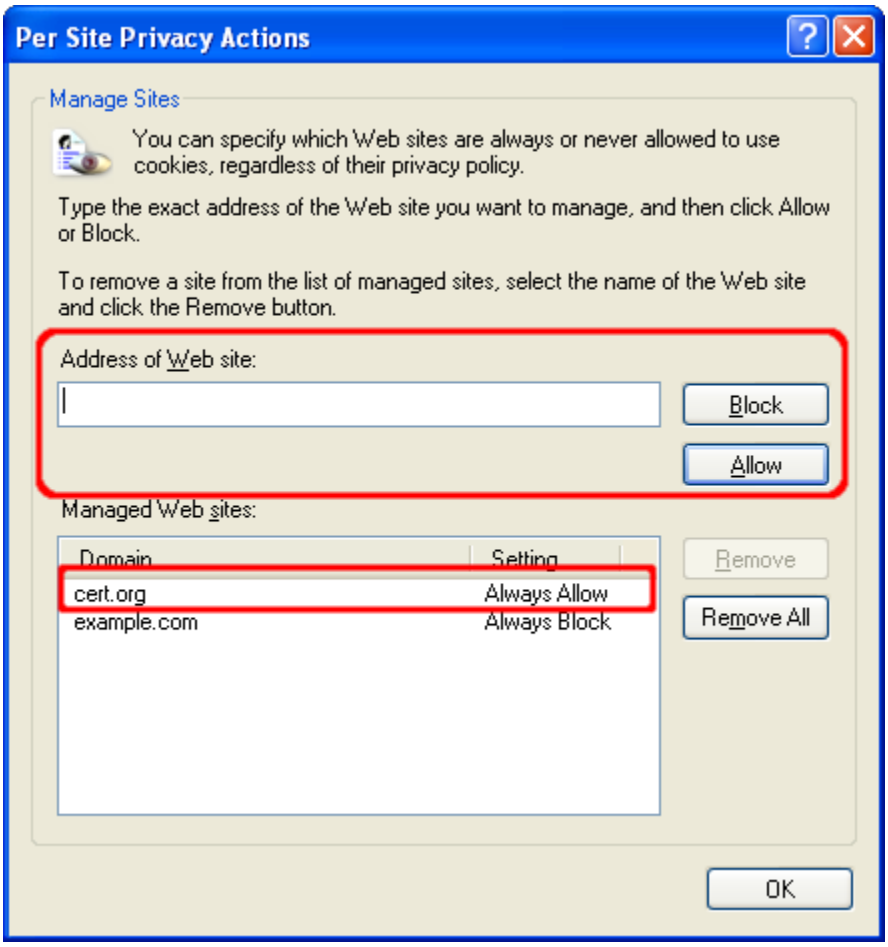
We recommend setting the security level for the **Trusted sites** zone to **Medium**. When the Internet Zone is set to **High**, you may encounter web sites that do not function properly due to one or more of the associated security settings. This is where the **Trusted sites** zone can help. If you trust that the site will not contain malicious code, you can add it to the list of sites in the Trusted sites zone. Once a site is added to this zone, features such as ActiveX and active scripting will be enabled. The benefit of this type of configuration is that IE will be more secure by default, and sites can be "whitelisted" in the Trusted sites zone to gain extra functionality.

The **Privacy** tab contains settings for cookies. Cookies are text files placed on your computer by various sites that you visit either directly (first-party) or indirectly (third-party) through ad banners, for example. A cookie can contain any data that a site wishes to store. It is often used to track your computer as you move through a web site and store information such as preferences or credentials.

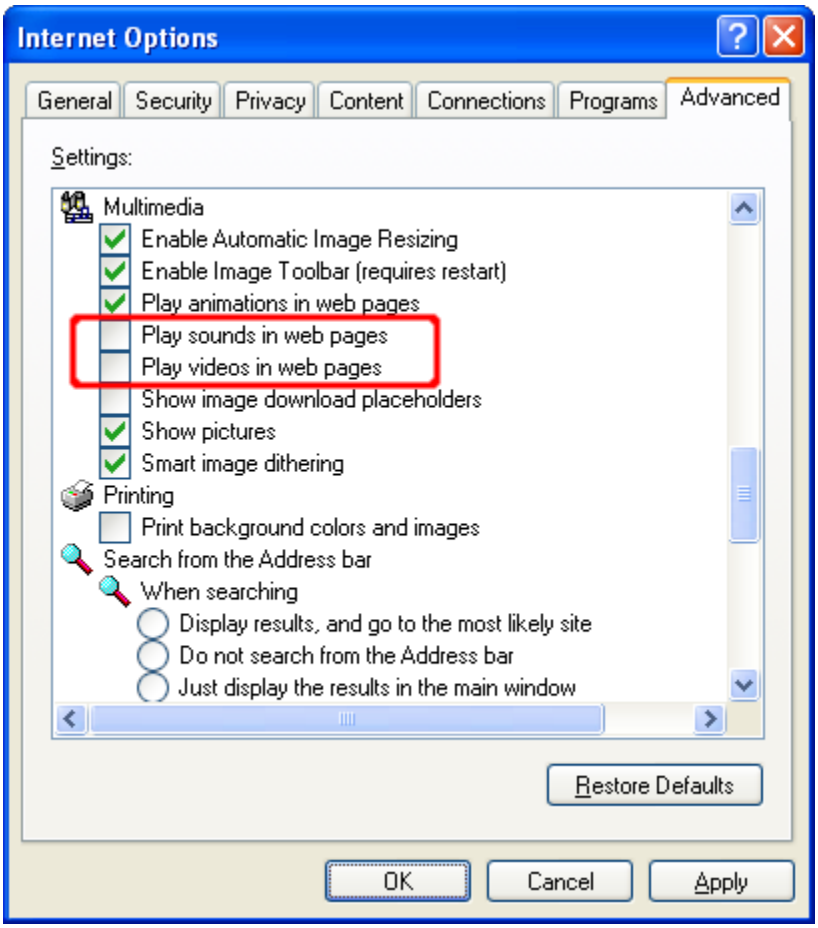


We recommend that you select the **Advanced** button and select **Override automatic cookie handling**. Then select **Prompt** for both first and third-party cookies. This will prompt you each time a site tries to place a cookie on your computer. You can then evaluate the originating site, whether you wish to accept or deny the cookie, and what action to take in the future (always accept, always block, or continue to ask).

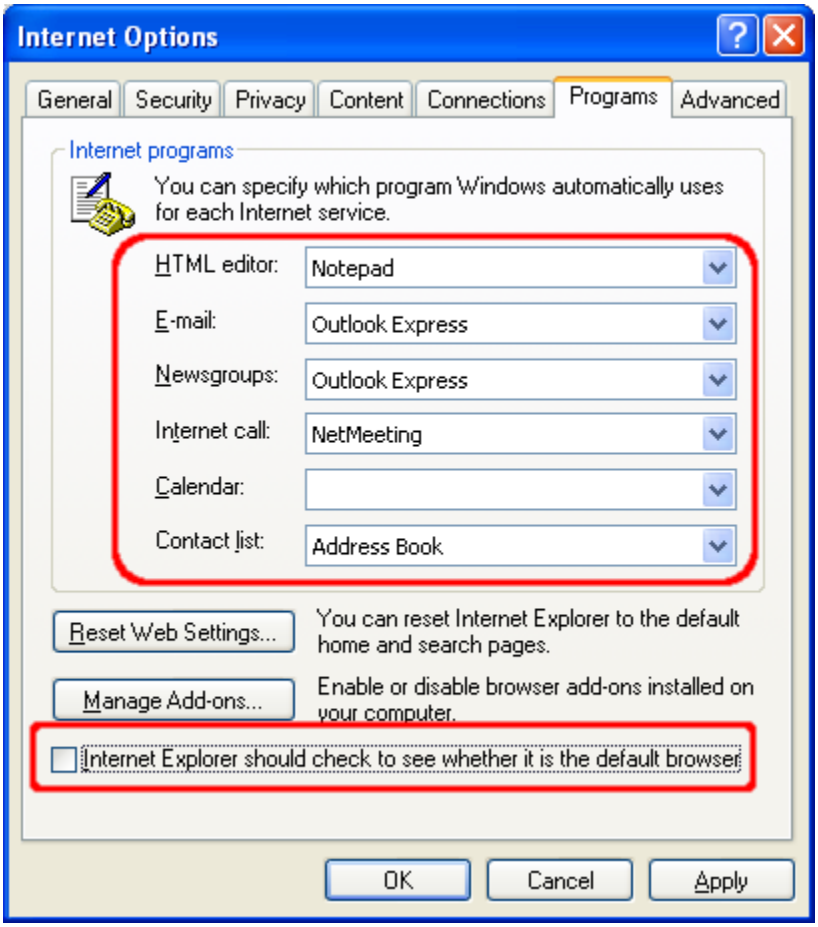
By selecting the **Sites...** button, you can manage the cookie settings for specific sites. You can add or remove sites, and you can change the current settings for existing sites. The bottom section of this window will specify the domain of the site and the action to take when that site wants to place a cookie on your computer. You can use the upper section of this window to change these settings.



The **Advanced** tab contains settings used by all zones. The settings contained in the **Multimedia** section have features that you can adjust to protect against some potential vulnerabilities. For instance, attackers may be able to track your usage or exploit the software you use to play multimedia data. We recommend disabling the options to play sounds and videos:



Under the **Programs** tab, you can specify your default applications for viewing web sites, email messages, and other network related tasks. You can also prevent Internet Explorer from showing you a message asking to be your default web browser.

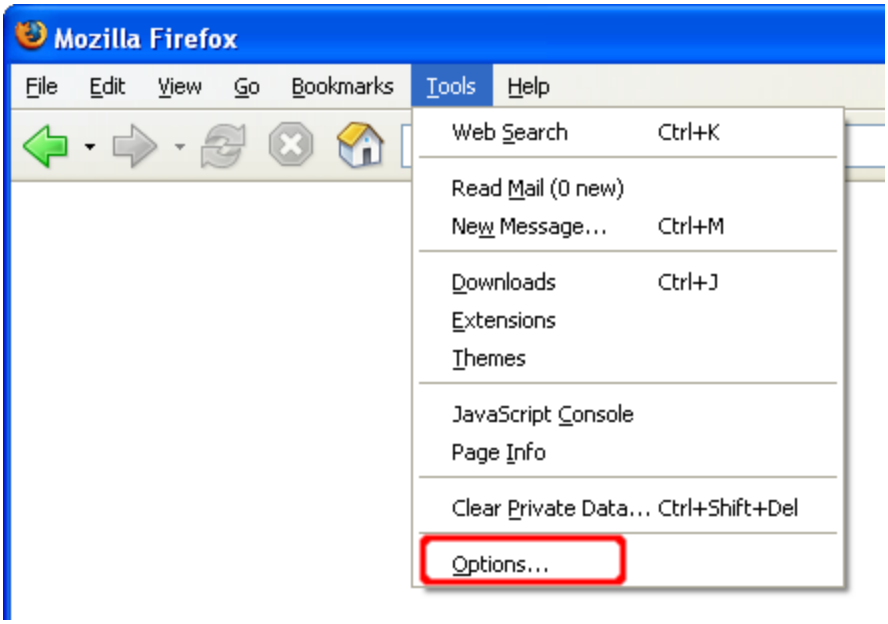


Mozilla Firefox

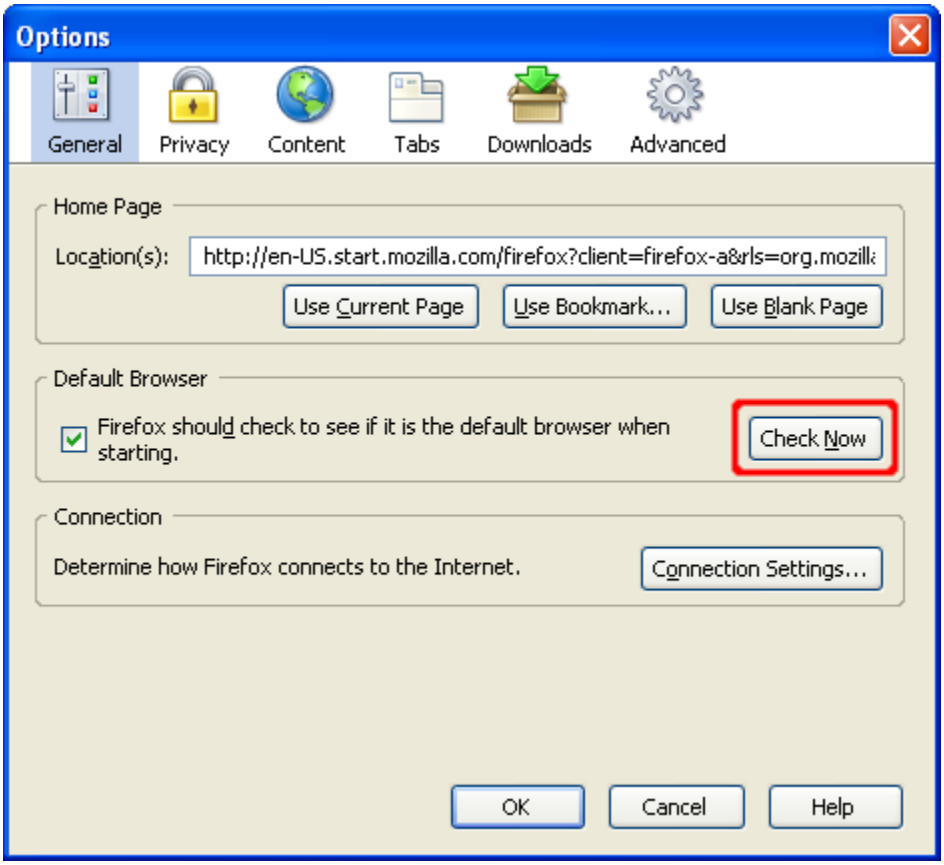
Mozilla Firefox supports many of the same features as Internet Explorer, with the exception of ActiveX and the Security Zone model. We recommend looking in the **Help**, **For Internet Explorer Users** menu to understand the different terminology used by the two browsers.

Following are steps to disable various features in Mozilla Firefox. Note that some menu options may change between versions or may appear in different locations depending on the host operating system. You should adapt the steps below as appropriate.

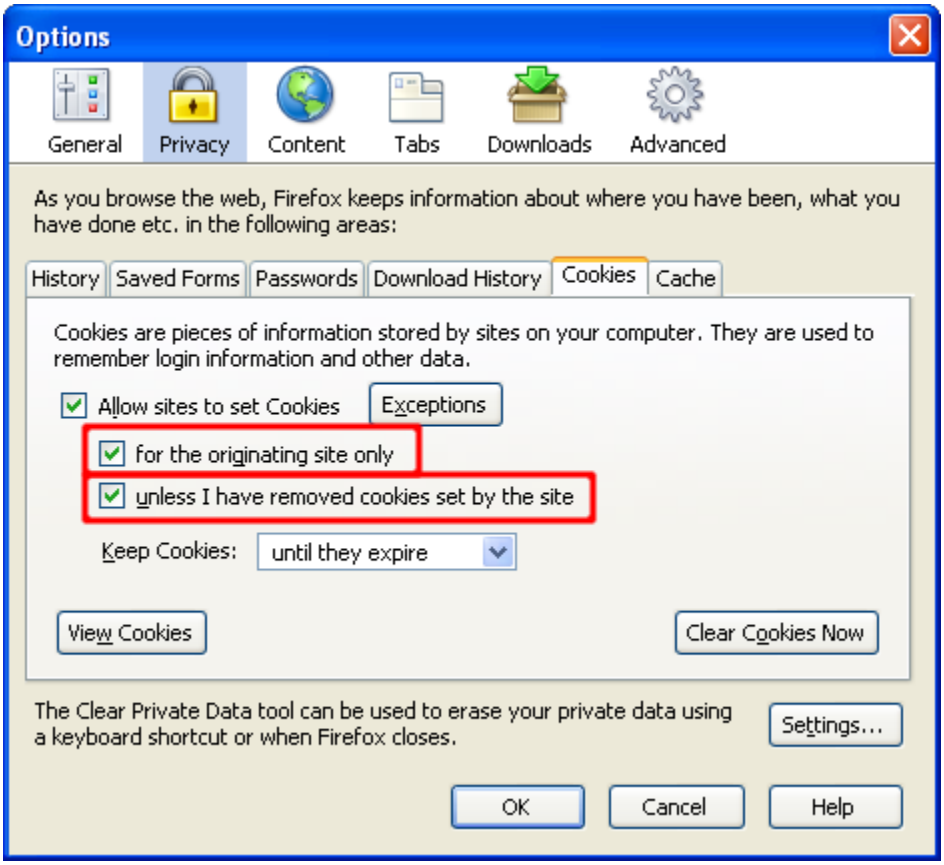
To edit the settings for Mozilla Firefox, select **Tools**, then **Options**.



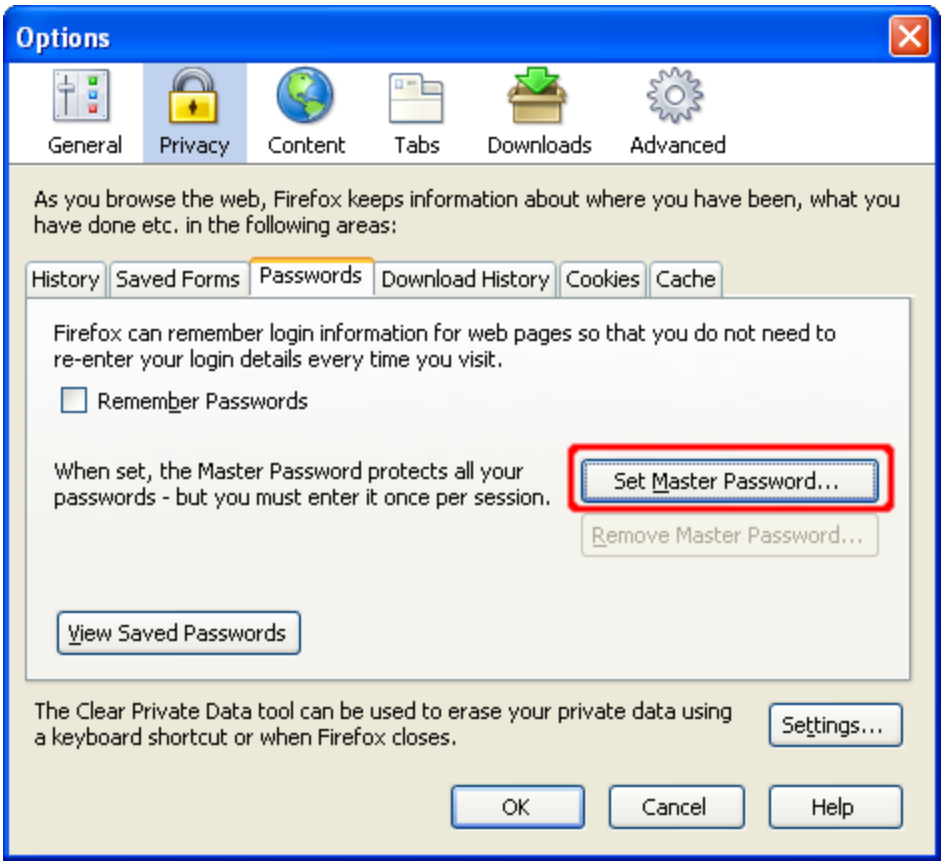
You will then see an Options window that has a row of categories along the top. The first category of interest is the **General** category. Under this section, for instance, you can set Firefox as your default browser.



Under the Privacy category, you can select the Cookies subcategory. Here you can disable cookies or change your preferences for how the browser handles them. In general, we recommend enabling cookies **for the original site only**. Additionally, by enabling the option **unless I have removed cookies set by the site**, a web site can be "blacklisted" from setting cookies when its cookies are removed manually.

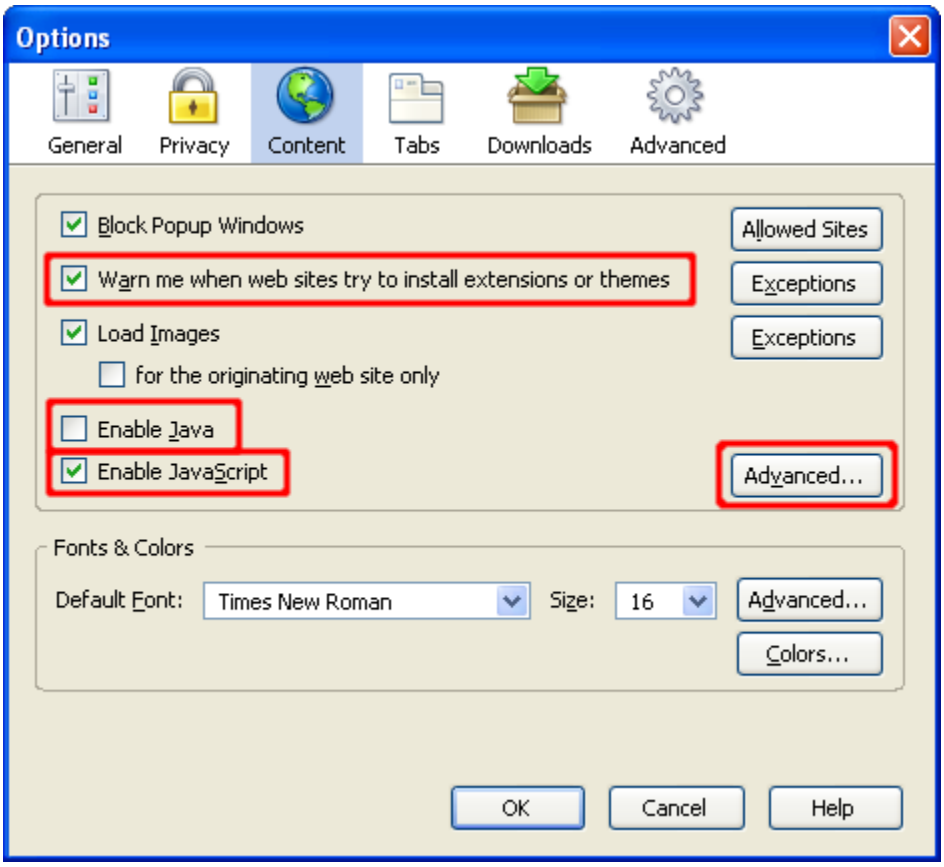


Many web browsers will allow you to store login information. In general, we recommend against using such features. Should you decide to use the feature, ensure that you use the measures available to protect the password data on your computer. Under the **Privacy** category, the **Passwords** subcategory contains various options to manage stored passwords, and a **Master Password** feature to encrypt the data on your system. We encourage you to use this option if you decide to let Mozilla Firefox manage your passwords.

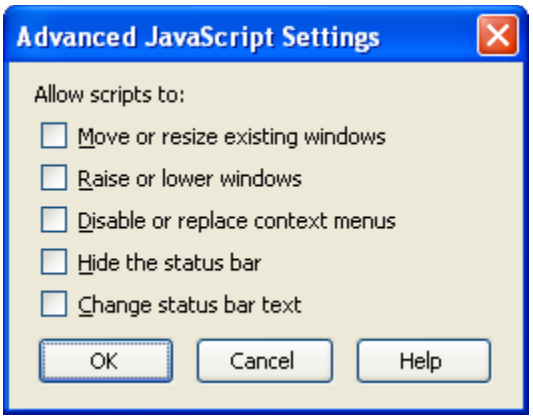


The **Content** category has an option to **Enable Java**. Java is a programming language that permits web site designers to run applications on your computer. We recommend disabling this feature unless required by the site you wish to visit. Again, you should determine if this site is trustworthy and whether you want to enable Java to view the site's content. After you are finished visiting the site, we recommend disabling Java until you need it again.

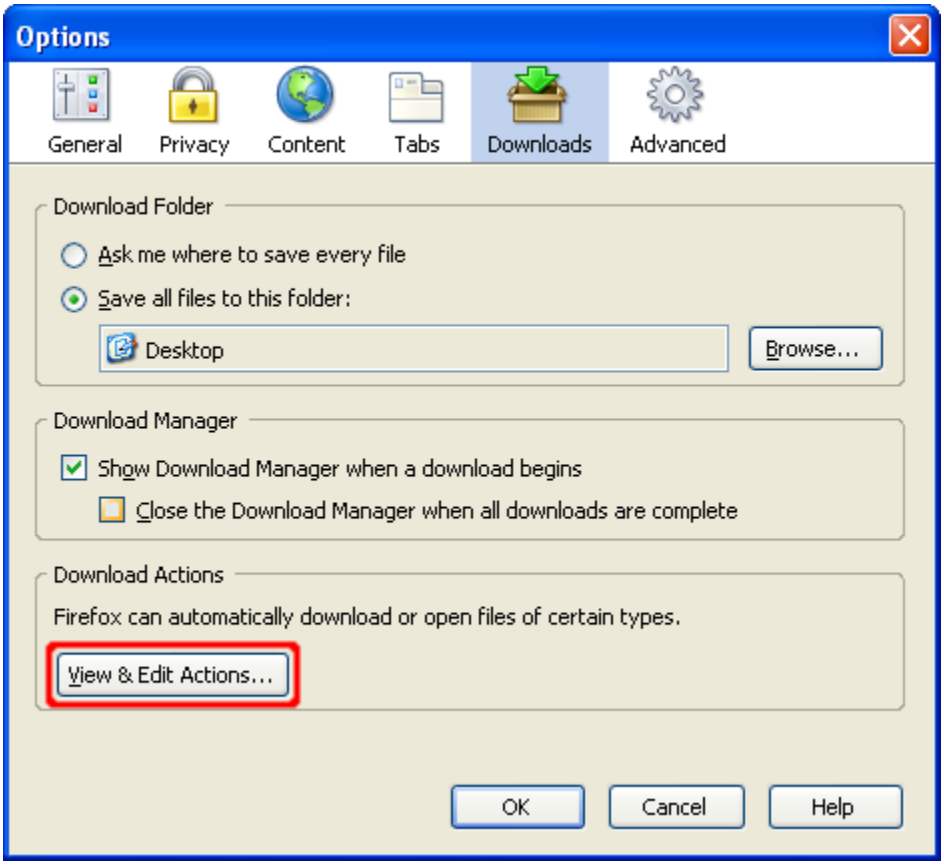
The **Warn me when web sites try to install extensions or themes** option will display a warning bar at the top of the browser when a web site attempts to take such an action.



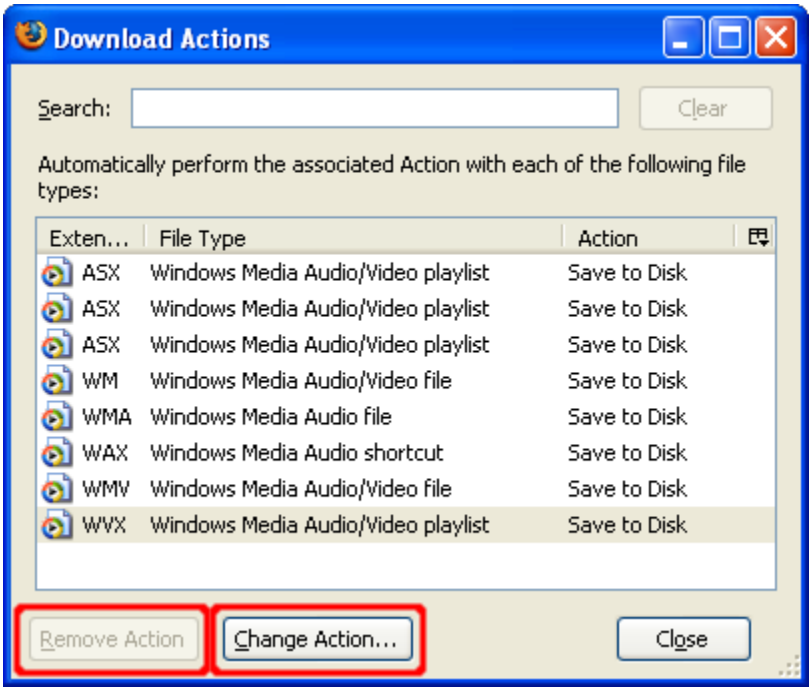
Press the **Advanced** button to disable specific JavaScript features. We recommend disabling all of the options displayed in this dialog.

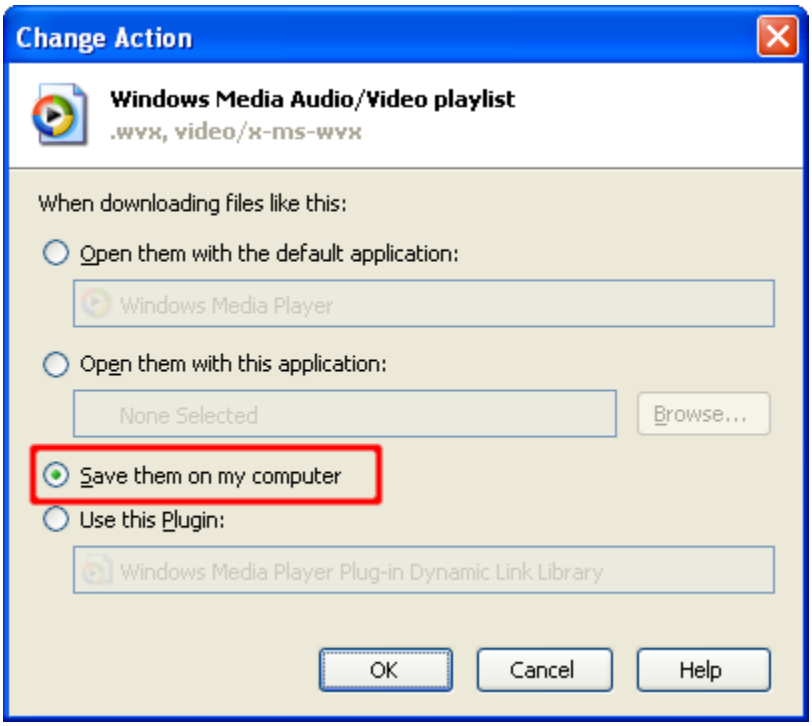


The **Downloads** section has an option to modify actions taken when files are downloading. Any time a file type is configured to open automatically with an associated application, this can make the browser more dangerous to use. Vulnerabilities in these associated applications can be exploited more easily when they are configured to open automatically. Click the **View & Edit Actions** button to view the current download settings and modify them if necessary.

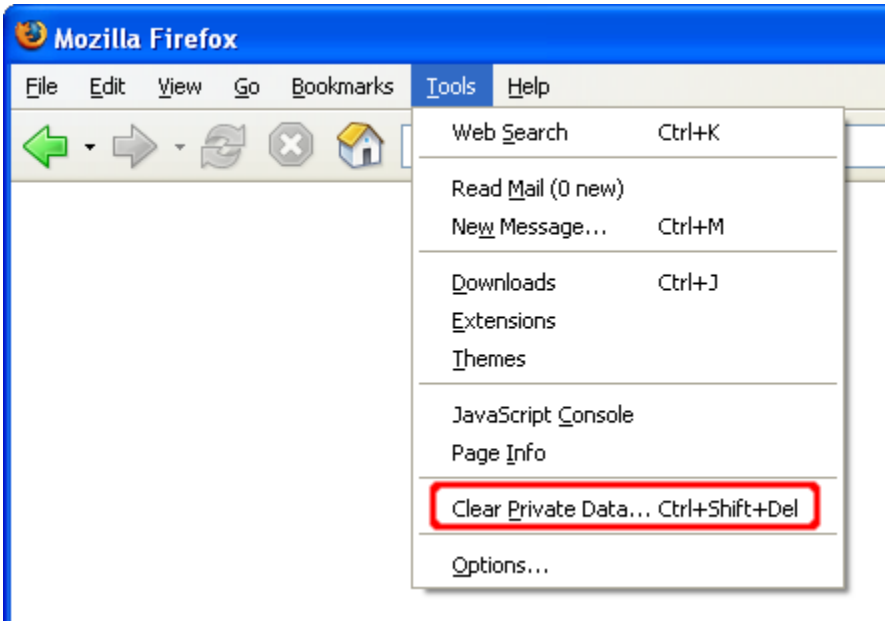


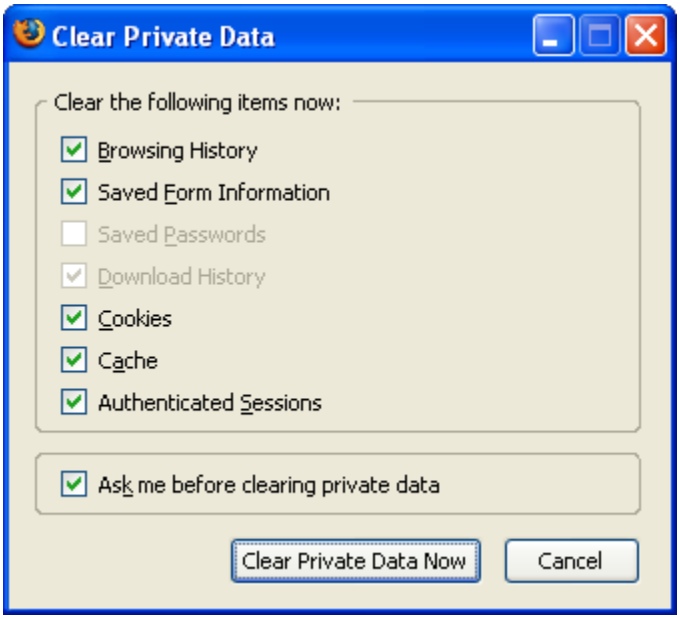
The Download Actions dialog shows the file types and the actions the browser will perform when it encounters a given file type. For any file type listed, click on either **Remove Action** or **Change Action...** . If you click on **Change Action...**, select Save them on my computer to save file of that type to the computer. This helps prevent automated exploitation of vulnerabilities that may exist in these applications.





Firefox 1.5 includes a feature to **Clear Private Data**. This option will remove potentially sensitive information from the web browser. Select **Clear Private Data...** from the **Tools** menu to use this privacy feature.



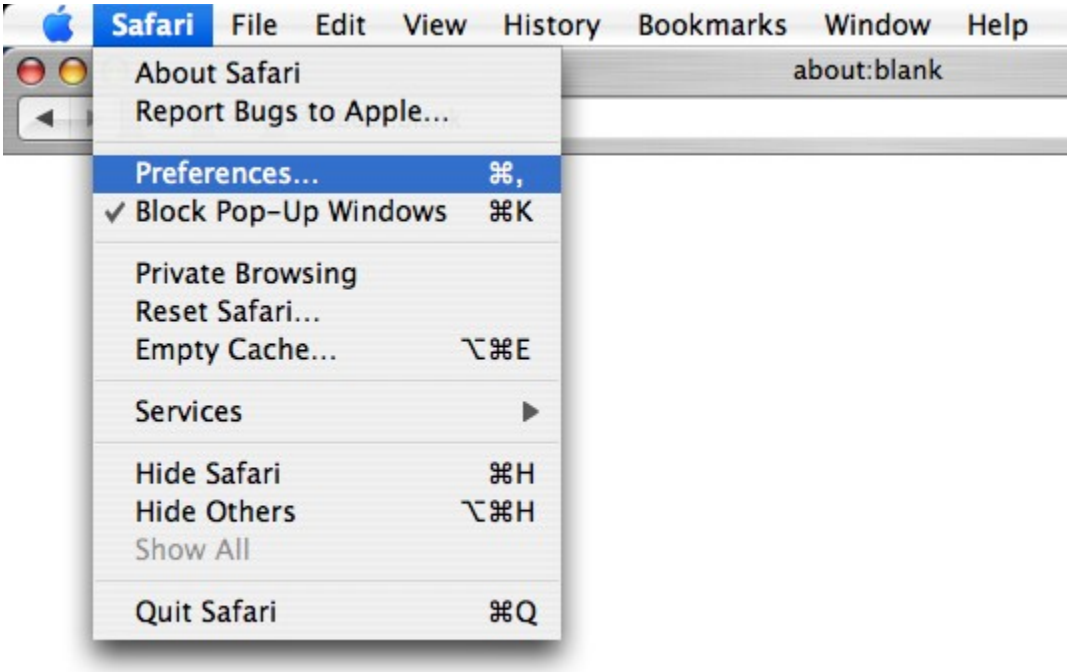


Apple Computer's Safari

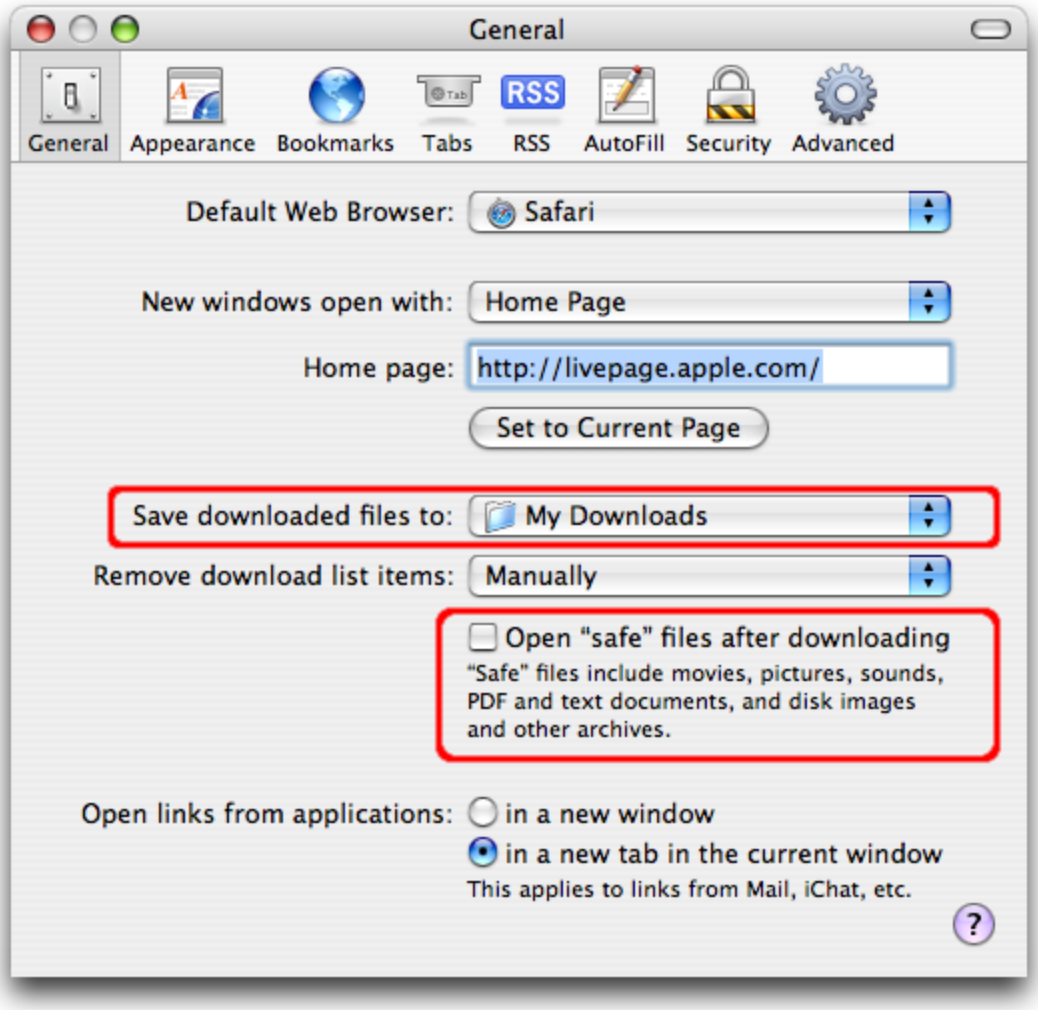
Safari supports many of the same features as Mozilla Firefox. This section describes steps to disable various features in Safari. Note that some menu options may change over time, and you should adapt the steps below as appropriate.

In order to change settings select **Safari** and then select **Preferences…**

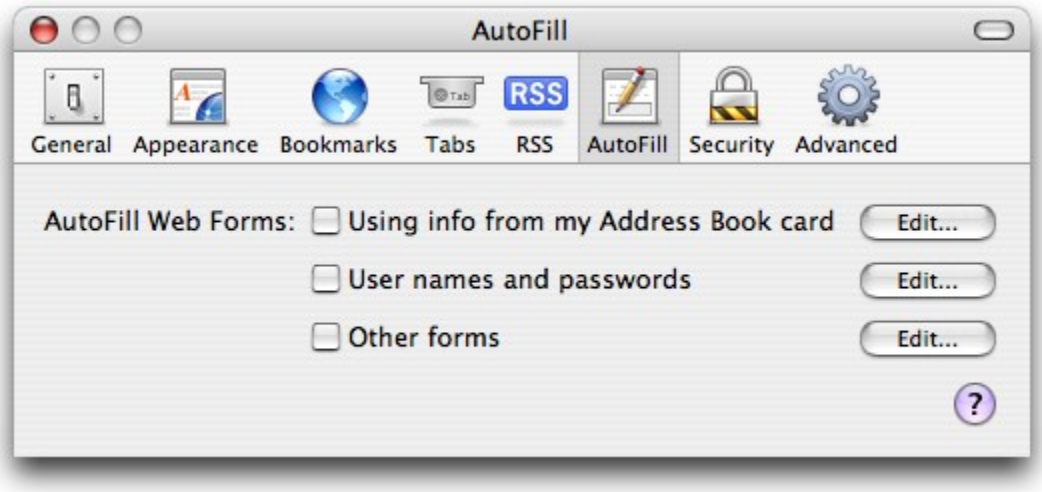
Note that on the Safari menu, you can also select the option "Block Pop-up Windows". This option will prevent sites from opening another window through the use of scripting, or active content. Be aware that while pop-up windows are often associated with advertisements, some sites may attempt to display content relevant to your usage of the site in a new window. Therefore, setting this option may disable the functionality of some sites.



Once you select the **Preferences** menu, the window depicted below will open. The first tab to examine is the **General** tab. On this tab, you can set up many options such as **Save downloaded files to:** and **Open "safe" files after downloading**. We recommend that you save downloaded files to a temporary folder that you create for downloading files. We also recommend that you deselect the **Open "safe" files after downloading** option.



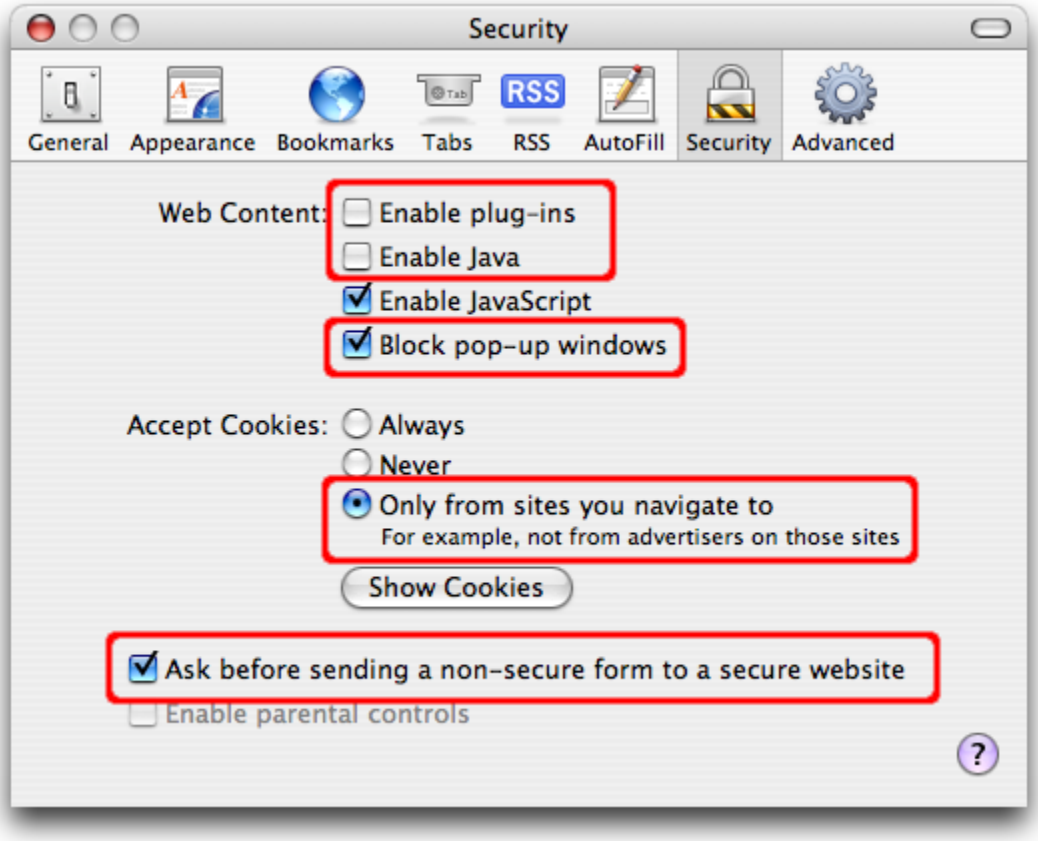
The next section of interest is the **AutoFill** tab. On this tab, you can select what types of forms your browser will fill in automatically. In general, we recommend against using AutoFill features. If someone can gain access to your computer, or to the data files, then the AutoFill feature may permit them even easier access to other sites that they would not otherwise have the ability to access. However, if used with appropriate protective measures, it may be acceptable to enable AutoFill. We recommend using filesystem encryption software such as OS X FileVault to provide additional security for files that reside in a user's home directory.



The **Security** tab provides several options. The **Web Content** section permits you to enable or disable various forms of scripting and active content. We recommend disabling the first three options in this section, and only enabling them when you require the functionality of these features. We recommend selecting the **Block Pop-up Windows** option. Remember that this option will prevent sites from opening another window through the use of scripting, or active content. Again, be aware that while pop-up windows are often associated with advertisements, some sites may attempt to display content relevant to your usage of the site in a new window. Therefore, setting this option may disable the functionality of some sites.

It is safer to use Safari without plug-ins and Java, so we recommend disabling the options **Enable plug-ins** and **Enable Java**. It is also safer to disable JavaScript. However, many web sites require JavaScript for proper operation.

In this dialog you can disable cookies and can also view or remove cookies that have been set. In general, we recommend disabling cookies and enabling them only when you visit a site that requires their use. At this point, you should determine if the site is trustworthy (i.e., contains no malicious content and is securely designed) and determine whether you want to allow cookies to access the site's content. After you are finished visiting the site, we recommend disabling cookies until you need to access a site that requires cookies. You can limit cookies to the sites that you navigate to by selecting the option **Only from sites you navigate to**. This will permit sites that you visit to set cookies, but not third-party sites. Finally, we recommend selecting the **Ask before sending a non-secure form to a secure website** option. This will alert when data is sent to a secure web site over an insecure channel.



Other Browsers

Other web browsers may have similar options to those described in the previous sections. Please refer to the browser documentation to determine which options are available and how to make the necessary changes. For example, here are some other popular browsers:

Mozilla Suite - http://www.mozilla.org/products/mozilla1.x
Opera - http://www.opera.com/support/tutorials/security
Konqueror - http://www.konqueror.org
Netscape - http://browser.netscape.com

Keeping Your Computer Secure

In addition to selecting and securing your web browser, you can take other steps to protect your computer:

A. Read the CERT/CC Home Network Security and Home Computer Security documents.

B. Install and use antivirus software

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Many antivirus packages support automatic updates of virus definitions. We recommend using these automatic updates when available. A partial list of antivirus vendors is available on the US-CERT web site.

C. Enable automatic software updates if available

Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation tells you how to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered, you may need to check the vendor's web site periodically for updates.

D. Avoid unsafe behavior

Additional information on this topic can be found in the document Home Network Security.

- Use caution when opening email attachments or when using peer-to-peer file sharing, instant messaging, or chat rooms.
- Don't enable file sharing on network interfaces exposed directly to the internet.

E. Follow the principle of least privilege — don't enable it if you don't need it

Consider creating and using an account with limited privileges instead of an 'administrator' or 'root' level account for everyday tasks. Depending on the operating system, you only need to use administrator-level access when installing new software, changing system configurations, and other important tasks. Many vulnerability exploits (e.g., viruses, Trojan horses) are executed with the privileges of the user that runs them — making it far more risky to be logged in as an administrator all the time.

References

US-CERT References

- Avoiding Social Engineering — http://www.us-cert.gov/cas/tips/ST04-014.html
- Browsing Safely: Understanding Active Content and Cookies — http://www.us-cert.gov/cas/tips/ST04-012.html
- Evaluating Your Web Browser's Security Settings — http://www.us-cert.gov/cas/tips/ST05-001.html
- Spyware — http://www.us-cert.gov/reading_room/spyware.pdf
- Understanding Internationalized Domain Names — http://www.us-cert.gov/cas/tips/ST05-016.html
- Understanding Web Site Certificates — http://www.us-cert.gov/cas/tips/ST05-010.html
- Understanding Your Computer: Web Browsers — http://www.us-cert.gov/cas/tips/ST04-022.html

CERT/CC References

- Before You Connect a New Computer to the Internet — http://www.cert.org/tech_tips/before_you_plug_in.html
- Home Computer Security — http://www.cert.org/homeusers/HomeComputerSecurity/
- Home Network Security — http://www.cert.org/tech_tips/home_networks.html
- Technical Trends in Phishing Attacks — http://www.cert.org/archive/pdf/Phishing_trends.pdf

Microsoft Windows XP References

- Improve the safety of your browsing and e-mail activities — http://www.microsoft.com/athome/security/online/browsing_safety.mspx
- Microsoft Windows XP Baseline Security Checklist — http://www.microsoft.com/technet/archive/security/chklist/xpcl.mspx
- Microsoft Windows XP Service Pack 2 — http://www.microsoft.com/windowsxp/sp2/default.mspx
- Microsoft's Protect Your PC — http://www.microsoft.com/protect/
- Setting Up Security Zones — http://www.microsoft.com/windows/ie/using/howto/security/setup.mspx
- Using the Internet Connection Firewall — http://www.microsoft.com/windowsxp/home/using/howto/homenet/icf.asp

Apple Macintosh OSX References

- Apple Product Security — http://www.apple.com/support/security/
- Apple Security Updates — http://docs.info.apple.com/article.html?artnum=61798
- How to Keep Network Computers Secure — http://docs.info.apple.com/article.html?artnum=61534
- OSX Security Features Overview — http://www.apple.com/macosx/features/security/

Linux References

- Debian Security Information — http://www.debian.org/security/
- Gentoo Security Handbook — http://www.gentoo.org/doc/en/security/
- Mandriva Security Advisories — http://www.mandriva.com/security/advisories
- RedHat Security and Errata — http://www.redhat.com/apps/support/errata/
- Slackware Security Advisories — http://www.slackware.com/security/
- SUSE Security (US/Canada) — http://www.novell.com/linux/security/securitysupport.html
- Ubuntu Security notices — http://www.ubuntu.com/usn/

System Administrator References

- Description of Internet Explorer security zones registry entries — http://support.microsoft.com/?kbid=182569
- How To Set Advanced Settings In Internet Explorer by Using Group Policy Objects — http://support.microsoft.com/?kbid=274846
- Internet Explorer Administration Kit — http://www.microsoft.com/technet/prodtechnol/ie/ieak